REMARKS/ARGUMENTS

A. THE CLAIMS

Claims 1-27 have been canceled. New claims 28-45 have been added and are pending in this application. No new matter has been added by these amendments.

B. CLAIM REJECTIONS

1. Generally

Examined claims 1-7, 9, 16-18, 20, 23, and 24 have been rejected under 35 U.S.C § 102(e) as being anticipated by Xu et al. U.S. Patent No. 6,738,362 (hereinafter, "Xu '362"). Claims 8, 10-12, 14, 19, 22 and 25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over '362 as applied to examined claims 1, 16, and 23 in further view of Liu et al., U.S. Patent No. 5,898,780 (herein, "Liu '780"). Claims 13, 15, 21, 26, and 27 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Xu '362 as applied to claims 1, 16, and 23 in further view of Liu '780, and in further view of Xu et al., U.S. Patent No. 6,151,628 (herein, "Xu '628").

2. Anticipation Rejections

Examined independent claim 1 was rejected as being anticipated by Xu '362. Examined independent claim 16 was rejected "along the same rationale" as examined independent claim 1.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP §2131 8th Ed. (Rev. 1). In order for a patent claim to be anticipated, the prior art reference must teach or suggest each and every limitation of the claimed invention.

Additionally, when applying a reference to the pending claims of an application, the pending claims must be "given their broadest reasonable interpretation consistent with the specification" *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). In *In re Morris*, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997), the court held that the "PTO applies to verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be

afforded by the written description contained in applicant's specification." The broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999). See, MPEP §2111 (8th Ed., Rev. 1). Applicant submits that if the pending claims of the present application are examined with full appreciation of the meaning ascribed to the terms used in the claims by the specification, it will become clear that the cited prior art does not teach the limitations of the pending claims.

A reference contains an "enabling disclosure" if the public was in possession of the claimed invention before the date of invention. "Such possession is effected if one of ordinary skill in the art could have combined the publication's description of the invention with his [or her] own knowledge to make the claimed invention." In re Donohue, 766 F.2d 531, 226 USPQ 619 (Fed. Cir. 1985).

As will be explained in detail below, the Xu '362 reference does not teach or described all of the limitations of the claimed inventions and does not enable one skilled in the art to make the claimed inventions. The Xu '362 reference cannot, therefore, support either an anticipation rejection or an obvious rejection of the pending claims. The Examiner referenced various sections of Xu '362 in finding that Xu'362 anticipated the examined claims. For convenience, these sections are presented in table form below.

Claim Limitation (As Examined)	Xu '362 Reference
Claim 1 - A method for dial roaming for users having a home non-LDAP (Lightweight Directory Access Protocol) region to allow access comprising: dialing into a local dial access provider; creating an access request; forwarding the dial access request...	[Xu '362, Col. 4, lines 14-25] In another aspect of the invention, a mobile Internet Protocol service provider system provides access to a network for a mobile node and enables the mobile node to communicate with a host on the network. The system-comprises a first communications device comprising a home registration agent responsive to a registration request message associated with the mobile node. The system further includes a second communications device, different from the first communications device, comprising a home tunneling agent associated with the home registration agent, the home tunneling agent receiving traffic from the mobile node and redirecting the traffic to the network.

Claim 1 - to a corporate remote authentication dial-in user service (RADIUS) server; proxying the request to a regional RADIUS server associated with the user's home region; accessing the regional user database to determine if the user is present in the regional database; authenticating the user; and providing configuration information to the user to allow access to the network.	[Xu '362, Col.4, line 55 through Col.5 line 25.] In yet another aspect, a method is provided for authenticating a mobile node for network access. In accordance with the method, a registration request message is generated and sent from a foreign agent to a home registration agent. The registration request message contains information used to determine whether said mobile node is authorized to access a network, such as the mobile device's unique International Mobile Subscriber Identity (IMSI) number and/or its Electronic Serial Number (ESN). The home registration agent then determines from the information in the registration request message whether the mobile node is permitted to access the network. This step may be performed with the assistance of a authorization, authentication and accounting server, e.g., a RADIUS server. The home registration agent then generates a registration reply message and sends the registration ;reply message from the home registration agent to the foreign agent. If the step of determining results in a positive response, i.e., that the mobile device is authenticated or registered to use the network, the home registration includes in the registration reply message a network address of a home tunneling agent. The home tunneling agent is adapted to receive data traffic from the mobile node and direct the traffic onto the network. The foreign agent forwards data traffic from the mobile node to the home tunneling agent for transmission to the host or destination. The home registration agent and the home tunneling agent are preferably implemented in two separate communications devices. Similarly, the foreign agent functionality may be split up into two separate devices, one functioning as a foreign tunneling agent and another device functioning as a foreign registration agent. The foreign and home registration agents exchange the registration and session control messages, while the tunneling activity is handled by foreign and home tunneling agents. These and still other features of the invention will be more apparent from the following detailed description of presently preferred and alternative embodiments of the invention.

Claim 2. The method for dial roaming of claim 1 wherein the access request is forwarded to an access provider via a network access server (NAS).	[Xu '362, Col. 3, Lines 41-48] In another related aspect of the invention, the functionality of a single foreign agent is distributed across multiple devices. For example, the registration and session control functions of a foreign agent are assigned to a first device, referred to herein as a "foreign registration agent", such as a general purpose computer or network access server on the visited network.
Claim 3. The method of claim 2 wherein the NAS functions as a client of the corporate RADIUS server.	[C 7, lines 39-45] The wireless communications service provider may furnish all the basic elements for providing mobile IP services, such as the foreign agents, and the home registration and home tunneling agents. Or, the entity may simply provide home tunneling and home registration agents, and work with other entities that own or manage the foreign agents.
Claim 4 - further comprising: the corporate RADIUS server determining if the user is a member of an LDAP or non-LDAP region	[Xu '362, Col. 7, lines 54-57] A number of different communications devices are all suitable platforms for implementation as a home registration agent. One example is a general-purpose computer. Another example would be an AAA or RADIUS server. Another example would be a router.
Claim 5 - wherein the determining if the user is a member of an LDAP or non-LDAP region is accomplished by reviewing a configuration file stored in the corporate RADIUS server.	[Xu '362, Col. 7, lines 59-67] In any event, the home registration agent 18A will typically comprise a machine having a central processing unit, an interface to a network, and a machine readable storage medium (such as EPROM, ROM or other type of memory device) containing a set of instructions for processing registration request messages associated with a mobile node and responsively generating registration reply messages. The details of a preferred registration reply message format are described in the next section.

Claim 6 - further comprising forwarding the access request to a regional LDAP database if the home region is LDAP enabled.	[Xu '362, Col. 8, lines 9-24] To support the separation of the home agent address and the home agent care-of-address during reverse tunneling (all data traffic that is bound for the home node is sent to the home tunneling agent and is tunneled by the home tunneling agent back to the mobile node via the foreign agent), a new extension as shown in FIG. 3 is defined. This extension will be carried inside a Mobile IP Registration Reply message when the mobile node 10 has been successfully authenticated. In the extension of FIG. 3, the four byte home agent care-of-address field 32 comprises the IP address of the home tunneling agent. The foreign agent tunnels traffic to this address as described above. If the extension of FIG. 3 does not appear in the Registration Reply message, the foreign agent must use the home registration agent IP address as the home agent care of address.
Claim 7. The method of claim 6 further comprising the regional LDAP database authenticating the user	As cited for claim 6.
Claim 8. The method of claim 7 further comprising the regional LDAP database sending an "accept" message if the user is in the regional LDAP database and a "deny" message if the user is not in the regional LDAP database.	[Liu '780, Col. 4, lines 50-65] Block 162 indicates that the server 136 includes software that attempts to match the "roaming" login information with an entry in a log table in the server 136. If the server 136 can make a match, then at block 166 the server 136 returns information to the server 132 that includes an IP address for a server that has the domain name contained in the login information provided by the user 144. The server 132 then sends an authentication request containing the user's name and password to the server 140. The server 140 checks this information and at block 170, transmits a message to the server 132 either stating that the user 144 should be granted or denied internet access. Block 174 indicates that if the server 136 cannot match the "roaming" login information, then a message is sent to the server 132 stating that internet access should be denied to the user 144.
Claim 9. The method of claim 1 wherein the access request comprises a user name and password.	[Xu '362, Col. 2, lines 21-24.] This may involve checking the identification of the mobile node (such as, through use of the mobile node's unique serial number or manufacturing number), password authentication, and possibly checking that the mobile node's account is current and paid in full.

Claim 10. The method of claim 9 wherein the user name comprises a regional naming convention for identifying the home region of the user.	[Liu '780, Col. 1, lines 25-27] In the method of the present invention, the user logs on to the local network of the foreign internet service provider using an identifier that includes the user's identification term, an identification term for the server of the home ISP....
Claim 11. The method of claim 9 wherein the user name comprises an email address of the user.	[Liu '780, Col. 1, lines 31-33] For example, the user might log on to the local network of the local ISP by using a standard e-mail address such as jdoe@aimnet.com, followed by the user's secret password.
Claim 12. The method of claim 9 further comprising comparing the user password to the password stored in the non-LDAP database.	[Liu '780, Col. 4, lines 50-61] Block 162 indicates that the server 136 includes software that attempts to match the "roaming" login information with an entry in a log table in the server 136. If the server 136 can make a match, then at block 166 the server 136 returns information to the server 132 that includes an IP address for a server that has the domain name contained in the login information provided by the user 144. The server 132 then sends an authentication request containing the user's name and password to the server 140. The server 140 checks this information and at block 170, transmits a message to the server 132 either stating that the user 144 should be granted or denied internet access.
Claim 13. The method of claim 12 wherein the password from the database is CHAP hashed, and wherein the password delivered to the database is CHAP hashed, and wherein the password comparison comprises comparing the CHAP hashed password delivered to the database with the CHAP hashed password extracted from the database.	[Xu '628, Col. 9, lines 48-57] In a preferred network access embodiment of the invention, a second phase authentication routine is employed to verify that the remote user is authorized to access the designated network. This is a accomplished by conducting a password authentication procedure such PAP or CHAP routine, both of which are known in the art, between either (1) the tunneling server 30 or (2) the authentication server 32A and the remote user, or (3) between authentication server 32A and tunneling server 30/34, thereby providing a second level of authentication.
Claim 14. The method of claim 12 wherein the database of the non-LDAP regions is an subscriber management system (SMS) database	[Liu '780, Col. 4, lines 50-51] Block 162 indicates that the server 136 includes software that attempts to match the "roaming" login information with an entry in a log table in the server 136.

Claim 15. The method of claim 9 wherein the password is hashed to maintain security.	[Xu '628, Col. 4, lines 45-54]. With this architecture, it is possible to divorce the location of the initial dial-up server (communications chassis 20) from the location at which the intermediate network terminates the dial-up protocol connection (PPP) and provides access to the target network 22 or 24 at the tunneling server 30. In addition to supporting the Internet 22 as the target network, this architecture also supports access to virtual private networks, allowing the remote wireless user to gain secure access to their corporate or private network such as the corporate enterprise network 24 illustrated in FIG. 1.
Claim 16. A system for dial roaming for users having a home non-LDAP region to allow access comprising: a user computer having a home service region for creating a network access request; a dial up connection over a first network to a network access server (NAS) in a roaming area: a second network connected to the NAS for receiving the network access request; a local network service provider connected to the second network; a third network connected to the network service provider; a corporate RADIUS server connected to the third network for receiving the access request; and a regional LDAP server comprising a user database for authenticating the user access request and for allowing access to the regional network.	See citations directed to claim 1.

Claim 17. The system of claim 16 further comprising a regional RADIUS server connected to a non-LDAP regional server connected to the second network for receiving the access request.	See claim 4.
Claim 18. The system of claim 17 wherein the non-LDAP regional server further comprises a user database and access instructions for authenticating the user access request in the non-LDAP server database.	[Xu '362, Col. 4, lines 45-49] includes a central processing unit, an interface to the network, and a machine readable storage medium comprising a set of instruction for processing registration request messages associated with the mobile node and responsively generating registration reply messages.
Claim 19. The system of claim 18 wherein the database is an SMS database.	See claim 14.
Claim 20. The system of claim 16 wherein the user access request comprises a user ID and password.	See claim 9.
21. The system of claim 20 wherein the NAS further comprises instructions for hashing the user ID and password to enhance security.	See claim 15.
22. The system of claim 18 wherein the non-LDAP server further comprises instructions to permit access if the user is in the database and to deny access if the user is not in the database.	See claim 8.

23. A system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database comprising: a RADIUS server, having a RADIUS authentication protocol, connected to a first network for receiving an access request from a user; a subscriber management server, connected to a second network, comprising a user database for authenticating the user access request over the second network; and a database view created in memory on the subscriber management server for providing user access information in the correct format for the RADIUS authentication protocol.	See claim 1.
24. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 23 wherein the user access request is a username and password.	See claim 9.
25. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 24 wherein the username is and email address.	See claim 11.

26. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 24 wherein the password from the user database is CHAP hashed to compare to the password presented in the user access request.	See claim 13.
Claim 27. The system for authenticating users using a standard RADIUS protocol against a non-standard subscriber management system and database of claim 26 wherein the subscriber management server further comprises instructions for sending an "accept" message to the RADIUS server if the user password from the user database matches the user password presented in the user access request, and for sending a "deny" message to the RADIUS server if the user password from the user database does not matche the user password presented in the user access request.	See claim 8.

Embodiments of the present invention are directed to permitting Internet users to roam outside of their home regions and to log on to their respective ISPs via dial-up networking. Ideally, a user's Internet Service Provider (ISP) would have implement a directory service compliant with the Lightweight Directory Access Protocol or LDAP. However, when this is not the case, logging on from outside the home region becomes problematic. Further, non-LDAP networks may be affiliated with other networks that are LDAP enabled. In such cases it is

difficult to verify that a user is authorized to use a non-LDAP network when the user is trying to access the network via dial-up connection. The present invention provides means for determining whether a user's home Internet service region is LDAP enabled and for employing alternative means to authenticate the user depending on the outcome of the determination.

By contrast, Xu '362 is directed to scaling network functionality among foreign agents and home agents:

> The present invention represents an improvement to the above approaches contemplated by the prior art. The present invention contemplates distributing the home agent functionality across multiple devices, with one device devoted to handing the registration and authentication functions, and another device devoted to the routing and tunneling functions of a home agent. The present inventors have appreciated that the: former functions, i.e., registration and authentication, are not particularly computationally intensive, and that a single general purpose computing device can handle a very large number of simultaneous registration and authentication transactions without any undue latency, management, or other problems, either alone or in concert with a RADIUS or Authorization, Authentication, and Accounting (AAA) server. On the other hand, the routing and inverse tunneling functions of a home agent are more CPU-intensive and better suited to more robust devices designed for such purposes, such as switches and routers. Thus, the present distributed home agent design of the present invention overcomes the scaling and management problems presented by prior art approaches and represents a simple, cost effective, and easily managed solution for providing mobile IP network services, particularly for large scale providers of such services. (Xu '362, Col. 3, lines 17-50.)

Thus, the present invention and Xu '362 are directed to solving significantly different problems. The present invention is not concerned with the computational issues associated with registration and authentication issues, but rather the structure (LDAP or non-LDAP) in which user identifying data is held. Xu '362 is not concerned with the datastructure in which the user identifying data is held and assumes that the foreign agent and home agent are compatible in this regard. Xu '362 acknowledges as much:

> The distribution of home agent functions between a home registration agent in one device and a home tunneling agent in another device works as follows. A mobile node 10 establishes a PPP connection with a foreign agent 16 over a wireless service provider network (not shown). The foreign agent 16 forwards a registration request message to the home registration agent 18A. The details of a registration request message are set forth in RFC 2002. The home registration agent 18A receives the registration request message and generates a registration reply message, indicating whether the mobile node 10 is allowed to access the

> network 26. The home registration agent may perform this authentication function alone, or, more preferably, with a separate AAA or RADIUS server 30. **The details of registration of a mobile node are not considered particularly important for the present invention and are known to persons skilled in the art.** (Xu '362, Col. 7, lines 2-12. Emphasis added by bolding.)

Newly added independent claim 28 recites the following limitations:

> 28. A method for dial roaming outside of a home service region comprising:
>
> dialing into a local dial access provider;
>
> creating an access request comprising user identifying information and home region identifying information;
>
> forwarding the access request to a corporate remote authentication dial-in user service (RADIUS) server;
>
> determining from the home region identifying information whether the home region supports Lightweight Directory Access Protocol (LDAP) authentication;
>
> if the home region does not offer LDAP authentication, then:
>
> proxying the access request to a regional RADIUS server associated with the user's home region;
>
> comparing the user identifying information in the access request with user identifying information stored in a regional user database accessible to the regional RADIUS server; and
>
> if the user identifying information in the access request matches the stored user identifying information, then:
>
> authenticating the user; and
>
> providing configuration information to the user to allow access to a network of the home region.

Claim 28 recites the limitations: "creating an access request comprising user identifying information and home region identifying information," and "determining from the home region identifying information whether the home region supports Lightweight Directory Access Protocol (LDAP) authentication."

The examiner found in examining claim 4 (now canceled) that Xu '362 teaches "determining from the home region identifying information whether the home region supports Lightweight Directory Access Protocol (LDAP) authentication" based on the following disclosure:

> A number of different communications devices are all suitable platforms for implementation as a home registration agent. One example is a general-purpose computer. Another example would be an AAA or RADIUS server. Another example would be a router. [Xu '362, Col. 7, lines 54-57]

The cited disclosure refers to a platform that may be employed to perform the tasks assigned to the home registration agent. The cited disclosure does not teach determining where to direct an access request based on the home region identifying information as taught by new claim 28 or now cancelled claim 4. Additionally, claim 28 describes a conditional authentication step not disclosed by Xu '362.

Because Xu '362 does not disclose all of the limitations of claim 28, claim 28 is not anticipated by Xu '362. Applicant respectfully submits that claim 28, as amended, is therefore allowable over Xu '362.

New claims 28-39 depend directly or indirectly from independent claim 28. Because claim 28 recites a limitation not found in Xu '362, claims 28-39 are allowable over Xu '362.

Independent claim 16 was rejected based on the same rationale as used to rejected examined claim 1. Applicant has added a new claim 40 that recites the following limitations:

> 40. A system for dial roaming outside of a home Internet service region comprising:
>
> a user computer having a home service region;
>
> a network access computer (NAC), wherein the NAC is adapted to:
>
> connect to the user computer via a dial-up connection;
>
> received user identifying information and home region identifying information from the user computer;
>
> create an access request comprising the user identifying information and the home region identifying information; and
>
> direct the access request to a corporate authentication dial-in user service (RADIUS) server; and
>
> the corporate RADIUS server, wherein the RADIUS server is adapted to:
>
> receive the access request;
>
> determine from the home region identifying information whether the home service region supports Lightweight Directory Access Protocol (LDAP) authentication; and
>
> if the home service region does not offer LDAP authentication, then proxy the access request to a regional RADIUS server

associated with the user's home region; and

the regional RADIUS server, wherein the regional RADIUS server is adapted to:

compare the user identifying information in the access request with user identifying information stored in a regional user database accessible to the regional RADIUS server; and

if the user identifying information in the access request matches the stored user identifying information, then authenticate the user and provide configuration information to the user computer to allow the user computer access to a network of the home region.

As with newly added claim 28, newly added claim 40 recites the limitation, "determine from the home region identifying information whether the home service region supports Lightweight Directory Access Protocol (LDAP) authentication." For the reasons previously outlined, this limitation distinguishes claim 40 over Xu '362.

Newly added claims 41-45 depend, directly or indirectly, on independent claim 40. Because claim 40 recites a limitation not found in Xu '362, claims 41-45 also recite a limitation not found in Xu '362 and are, therefore, allowable over Xu '362.

3. Obvious Rejections

Claims 8, 10-12, 14, 19, 22 and 25 have been rejected under 35 U.S.C. 103(a) as being unpatentable over '362 as applied to examined claims 1, 16, and 23 in further view of Liu et al., U.S. Patent No. 5,898,780 (herein, "Liu '780"). Claims 13, 15, 21, 26, and 27 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Xu '362 as applied to claims 1, 16, and 23 in further view of Liu '780, and in further view of Xu et al., U.S. Patent No. 6,151,628 (herein, "Xu '628").

As previously discussed, the newly added claims include at least one limitation not taught or disclosed by the Xu '362. The examiner did not find the common limitation of the newly added independent claims, "determining from the home region identifying information whether the home region supports Lightweight Directory Access Protocol (LDAP) authentication," in any of the other cited references. Thus, the combinations proffered by the examiner do not include this limitation. For this reason, claims 29-39 that depend, directly or indirectly, from newly added claim 28 and claims 41-45 that depend, directly or indirectly, from newly added claim 40

are allowable over the cited references.

Applicant respectfully requests reconsideration of the current rejection. In view of the responses and remarks made above, Applicant further requests issuance of a timely Notice of Allowance in this case. Should any further questions arise concerning this application or in the event the above amendments do not place the application in condition for allowance, Applicant respectfully requests a telephone interview. Please contact Jon Roberts at the number listed below.

Respectfully Submitted,

By 

Jon L. Roberts
Reg. No. 31,293
Elliott D. Light
Reg. No. 51,948
Roberts Abokhair & Mardula, LLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191
703-391-2900